US009594827B2

(12) **United States Patent**
Ghafourifar et al.

(10) **Patent No.: US 9,594,827 B2**
(45) **Date of Patent: Mar. 14, 2017**

(54) **SYSTEM AND METHOD OF DYNAMIC, ENCRYPTED SEARCHING**

(71) Applicant: **Entefy Inc.**, Palo Alto, CA (US)

(72) Inventors: **Alston Ghafourifar**, Los Altos Hills, CA (US); **Philip Nathan Greenberg**, San Diego, CA (US); **Mehdi Ghafourifar**, Los Altos Hills, CA (US)

(73) Assignee: **Entefy Inc.**, Palo Alto, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/985,907**

(22) Filed: **Dec. 31, 2015**

(65) **Prior Publication Data**

US 2016/0179938 A1 Jun. 23, 2016

Related U.S. Application Data

(63) Continuation-in-part of application No. 14/579,712, filed on Dec. 22, 2014.

(51) **Int. Cl.**

G06F 7/02	(2006.01)
G06F 17/30	(2006.01)
G06F 21/62	(2013.01)
H04L 12/58	(2006.01)

(52) **U.S. Cl.**

CPC .. ***G06F 17/30616*** (2013.01); ***G06F 17/30106*** (2013.01); ***G06F 17/30321*** (2013.01); ***G06F 17/30675*** (2013.01); ***G06F 17/30864*** (2013.01); ***G06F 21/6227*** (2013.01); ***H04L 51/066*** (2013.01); ***H04L 51/16*** (2013.01); *H04L 51/36* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,481,597 A	1/1996	Given
5,951,638 A	9/1999	Hoss
6,101,320 A	8/2000	Schuetze

(Continued)

FOREIGN PATENT DOCUMENTS

WO	9931575	6/1999
WO	2013112570 A1	8/2013

Primary Examiner — Bruce Moser

(74) *Attorney, Agent, or Firm* — Blank Rome LLP

(57) **ABSTRACT**

This disclosure relates to personalized and dynamic server-side searching techniques for encrypted data. Current so-called 'zero-knowledge' privacy systems (i.e., systems where the server has 'zero-knowledge' about the client data that it is storing) utilize servers that hold encrypted data without the decryption keys necessary to decrypt, index, and/or re-encrypt the data. As such, the servers are not able to perform any kind of meaningful server-side search process, as it would require access to the underlying decrypted data. Therefore, such prior art 'zero-knowledge' privacy systems provide a limited ability for a user to search through a large dataset of encrypted documents to find critical information. Disclosed herein are communications systems that offer the increased security and privacy of client-side encryption to content owners, while still providing for highly relevant server-side search-based results via the use of content correlation, predictive analysis, and augmented semantic tag clouds for the indexing of encrypted data.

25 Claims, 18 Drawing Sheets